IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for assembling fragmented network traffic, comprising:

detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;

initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and

performing further processing on the fragmented network traffic having the anomaly; wherein performing further processing comprises determining configuration information associated with how the destination node is configured to reassemble overlapping fragments.

2. (Original) A method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap.

3. (Original) A method as recited in claim 2 wherein determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments.

4. (Original) A method as recited in claim 3 wherein the header value comprises an offset value.

5. (Original) A method as recited in claim 1 wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments.

6. (Cancelled)

7. (Original) A method as recited in claim 6 wherein determining configuration information comprises querying the destination node.

8. (Original) A method as recited in claim 6 wherein determining configuration information comprises querying an information base.

9. (Original) A method as recited in claim 1 wherein performing further processing comprises reassembling the fragmented network traffic to generate more than one variant of the reassembled data flow.

10. (Original) A method as recited in claim 1 further including processing the anomaly to determine whether the fragmented network traffic is associated with a threat.

11. (Original) A method as recited in claim 1 further including performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat.

12. (Original) A method as recited in claim 1 further including discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat.

13. (Original) A method as recited in claim 1 further including copying one or more fragments comprising the fragmented network traffic to a buffer.

14. (Original) A method as recited in claim 1 wherein performing further processing comprises sending an alert.

15. (Original) A method as recited in claim 1 wherein performing further processing comprises determining whether the fragmented network traffic should be blocked.

16. (Original) A method as recited in claim 1 wherein performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node.

17. (Canceled)

18. (Previously presented) A method as recited in claim 1 wherein detecting an anomaly comprises determining that two or more fragments contained in said fragmented network traffic have overlapping portions.

19. (Previously presented) A method as recited in claim 1 wherein detecting an anomaly comprises determining that two or more fragments contained in said fragmented network traffic have mismatching overlapping portions.

20. (Currently amended) A system for assembling fragmented network traffic, comprising:

a memory configured to store at least a portion of the fragmented network traffic; and

a processor configured to:

detect in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;

initiate in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and

perform further processing on the fragmented network traffic having the anomaly;

wherein performing further processing comprises determining configuration information associated with how the destination node is configured to reassemble overlapping fragments.

21. (Currently amended) A computer readable storage medium ~~program product for assembling fragmented network traffic, the computer program product being embodied in a computer readable storage medium and~~ comprising computer instructions for assembling fragmented network traffic, including instructions for:

detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed;

initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and

performing further processing on the fragmented network traffic having the anomaly;

wherein performing further processing comprises determining configuration information associated with how the destination node is configured to reassemble overlapping fragments.

22. (New) The system of claim 20 wherein determining configuration information comprises querying the destination node.

23. (New) The system of claim 20 wherein determining configuration information comprises querying an information base.